

**TERRORISM PLANNING COURSE
TOOLKIT¹
VERSION 3 (MARCH 2002)**

APPENDIX D: CYBERTERRORISM

Ours is an age of computers, of automated information systems. We are able to access, distribute, and store incredibly large quantities of information in very little time. It is said that information is power. However, our dependence on automated information systems goes much deeper than power-wielding. Virtually all of the infrastructure and the institutions on which we depend—the government, military, communications systems, transportation, utilities, financial systems, emergency medical services, and more—depend on automation. ...

As we have harnessed automation and created systems to facilitate and quicken our private, corporate, and governmental transactions, those systems have become increasingly vulnerable. We now face the danger of having our information infrastructures destroyed, altered, or incapacitated. Too often those vulnerabilities go unnoticed until disruption or catastrophe occurs.

Attacks on our information systems may come from a wide range of potential aggressors, from other nations to teenage hackers. One of the greatest threats comes from cyberterrorism.

WHAT IS CYBERTERRORISM?

Cyberterrorism is the convergence of cyberspace (the computer-based world of information) and terrorism (premeditated, politically motivated violence perpetrated against noncombatant targets by sub-national groups or clandestine agents).

The boundaries of cyberterrorism—what does and what does not constitute an act of cyberterrorism—are variously defined. Here is one definition:

Definition: Cyberterrorism

Unlawful attacks and threats of attack against computers, networks, and the information stored therein when done to intimidate or coerce a government or its people in furtherance of political or social objectives.

Further, to qualify as cyberterrorism, an attack should result in violence against persons or property, or at least cause enough harm to generate fear. Attacks that lead to death or bodily injury, explosions, or severe economic loss would be examples. Serious attacks against critical infrastructures could be acts of cyberterrorism, depending on their impact. Attacks that disrupt nonessential services or that are mainly a costly nuisance would not.²

Cyberterrorism is distinct from computer crime, economic espionage, and "hactivism," although terrorists may employ any of these forms of computer abuse to further their agendas.

¹ http://www.fema.gov/txt/onp/toolkit_app_d.txt

² Denning, Dorothy E., "Cyberterrorism." August 2000. Prepublication version of a paper that appeared in *Global Dialogue*, Autumn 2000.

The weapons of cyberterrorism—computers—differ from weapons of mass destruction such as biological agents, chemical agents, and radiological agents in that they don't directly cause death and injury. However, acting indirectly, they can cause serious consequences to individuals, businesses, industry, government, and the public at large. Depending on how they are used, they can lead to injury and death.

To better understand cyberterrorism, it is helpful to understand the terminology that has been coined to describe this growing phenomenon. The following table provides a few key definitions related to cyberterrorism.

SOME GENERAL TERMS RELATED TO CYBERTERRORISM³

...

cyberterrorism

Computer-based, information-oriented terrorism.

cyberwar

Information-oriented warfare waged by formal military forces.

cybotage

Acts of disruption and destruction against information infrastructures; computer sabotage.

cyboteur

One who commits cybotage; anarchistic or nihilistic computer hacker; computer saboteur.

hacking

Breaking into computer networks.

WHY CYBERTERRORISM?

Cyberterrorism is the weapon of the weak. It appeals to fringe groups who cannot match the military might of their "oppressors" or perceived enemies. Many terrorist organizations aim to achieve a new "future order" if only by wrecking the present. There are several factors that make cyberterrorism an attractive weapon for terrorists:

* Vulnerability: The very linkages that enable information technology (IT) systems to function also provide vulnerable points that can be exploited by terrorists. Our sheer dependence on the systems' functioning as planned is a source of great vulnerability.

...

* Availability and low cost: Availability of the weapons of cyberterrorism and the potential for disruptive effects are rising, while financial and other costs are decreasing. A wide array of easy-to-use software attack tools is readily available without cost from thousands of web sites. For a minimum investment, attacks can be waged that are serious and costly; the terrorists can affect more people at less risk to themselves than with other types of terrorist weapons. "Tomorrow's terrorist may be able to do more damage with a keyboard than with a bomb."⁴

³ From "Terrorism Evolves Toward Netwar," in *Rand Review*, Winter 1998-99 issue; and Denning, Dorothy E., "Activism, Hactivism, and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy," in Networks and Netwars: The Future of Terror, Crime, and Militancy. Arquilla, John, and Ronfeldt, David, eds. Rand Corp., 2001. Both accessed at www.rand.org/publications/randreview/issues/rrwinter98.9/madness.html.

⁴ National Research Council, "Computers at Risk," *National Academy Press*, 1991.

...

* Expertise: In the last few years, many automated attack tools have appeared on the Internet, making it much easier even for ignorant attackers to cause considerable damage. However, new generations of hackers are growing up with ever more digital capability, and hacker networks are already huge. Hackers and insiders might be recruited by terrorists or become self-recruiting cyberterrorists.

...

These factors make cyberterrorism an appealing weapon and increase the likelihood that cyberterrorism will only increase in the future. U.S. experts are justifiably concerned about our vulnerability to this type of attack. According to the Center for Strategic and International Studies in Washington, DC, "Cyberterrorists, acting for rogue states or groups that have declared holy war against the United States, are known to be plotting America's demise as a superpower."⁵

METHODS OF ATTACK

RISK FACTORS

There are three key risk factors related to computer systems: access, integrity, and confidentiality.

The proper functioning of information systems is predicated on restricted access to data and operations, on the integrity (accuracy and timeliness) of the data, and on the confidentiality of information that is intended to remain private.

If unauthorized parties gain access to a system, they can cause damaging actions to occur within the system. If a database is accessed and manipulated, the ripple effect can be enormous; the smallest change in a database can cause huge damage (change one number, and all resulting data becomes unreliable).

If confidentiality is breached, private information may become public and sensitive data may fall into the wrong hands. Theft of passwords and user IDs can enable unauthorized access, and the cycle continues.

TYPES OF CYBERTERRORISM

The following are some general types of cyberterrorism:

* Data destruction or corruption: Using viruses, installation of malicious code, or other means to damage a system from within. This could include destroying or corrupting files, changing data in a database, or corrupting software programs within the system.

* Penetration of a system to modify its output: Embedding code (e.g., Trojan horses or "logic bombs") to perform unauthorized functions at a later time.

* Theft: System penetration with the goal of stealing information or sensitive data (e.g., password cracking and theft, "packet sniffing").

* Disabling a system: Disruption of information structures (e.g., using e-mail bombings, spamming, denial-of-service attacks, or viruses) to crash or disable a system.

* Taking control of a system: Taking over a system (e.g., an air traffic system, a manufacturing process control system, a subway or train system, a 911 communications system) to use it as a weapon.

* Website defacement: Hacking into a website and changing its contents to spread misinformation, incite to

⁵ Global Organized Crime Project, *Cybercrime, Cyberterrorism, and Cyberwarfare*. Center for Strategic and International Studies, 1998.

violence, generate fear, or create chaos.

Terrorist groups also use websites, chat rooms, and encrypted e-mail to plan physical acts of terrorism, raise funds for terrorism, provide instructions to fellow terrorists, provide instructions on how to build bombs, spread hate propaganda, and recruit members.

SOME TOOLS OF CYBERTERRORISM

The following table describes some of the tools that can be used by cyberterrorists to cause disruption and damage.

Cyberterrorism Tools

TOOL

DESCRIPTION

HERF Gun

High Energy Radio Frequency Gun. Directs a blast of high energy radio signals at a selected target to disable it, at least temporarily. A HERF Gun can shoot down a computer, cause an entire network to crash, or send a telephone switch into electronic chaos. Any of these effects can create denial-of-service scenarios. A HERF Gun is simple and easy to build.

EMP/T Bomb

Electromagnetic Pulse Transformer Bomb. Operates similarly to a HERF Gun, but is many times more powerful and causes permanent damage. According to a 1980 FEMA report⁶, the following hardware would be most susceptible to failure from EMP:

- * Computers, computer power supplies, and transistorized power supplies.
- * Semiconductor components terminating long cable runs (especially between sites).
- * Alarm systems and intercom systems.
- * Life support system controls.
- * Telephone equipment.
- * Transistorized receivers, transmitters, and process control systems.
- * Power control systems.
- * Communications links.

Detonated over a dense urban area, EMP/T Bombs could take out all communications and electronic equipment and cause a blackout.

System intrusion

Unauthorized entry into a system (hacking). Can be used for information gathering, information alteration, and sabotage.

Emissions capture

Various tools are available for capturing vital information secrets such as passwords or data. Packet sniffing (below) is one approach. Van Eck emissions enable hackers to capture the contents of computer screens from up to 200 meters away. Devices designed to capture these emissions can be developed at very low cost.

Virus

A program that can attach itself to legitimate files and propagate, spreading like an infectious disease from computer to computer as files are exchanged between them. The virus hides until a certain criterion is met, then attacks the system by erasing files, destroying hard disk drives, or corrupting databases.

Worm

⁶ FEMA. EMP Threat and Protective Measures. Report for public distribution. April 1980, p. 11.

Operates much like a virus but can travel along a network on its own.

Trojan horse

A program that pretends to be a benign program but is really a program of destruction. When the user runs the program, it can perform the same kind of destruction as a virus.

E-mail bombing

Flooding a site with so many e-mails that the system becomes paralyzed.

Logic bomb

Unauthorized code that creates havoc when a particular event occurs, such as a certain date.

Packet sniffing

Installing a software program on a network that monitors packets sent through the system and captures those that contain passwords and user IDs.

Spamming

Flooding a system with massive numbers of a message.

Sustainable pulsing

Repeated convergence, redispersion, and recombination of small, dispersed, internettted forces against a succession of targets.

Swarming

Unleashing multiple attacks on a cyberspace target from all directions at once.

Denial-of-service attack

Causing internal damage to a server, or overloading a site with "hits," to the extent that service is denied to authorized users.

Web sit-in

Mass convergence on a website to overload the site (e.g., with rapid and repeated download requests).

POTENTIAL TARGETS OF CYBERTERRORISM

Of greatest concern for emergency planners are terrorist attacks intended to interfere with national life support systems. Systems of greatest priority include:

- * Telecommunications.
- * Banking and finance.
- * Electrical power.
- * Oil and gas distribution and storage.
- * Water supply.
- * Transportation.
- * Emergency services.
- * Government services.

Even worse would be the simultaneous occurrence of a physical act of terrorism, such as release of a chemical or biological agent or detonation of a radioactive device, and an act of cyberterrorism that would interfere with response capabilities.

POSSIBLE CYBERTERRORISM SCENARIOS

Many potential scenarios for cyberattacks have been suggested, and there are undoubtedly many more that are equally possible. The following are some of the scenarios that have been discussed in cyberterrorism literature, along with selected examples of actual events that have occurred. Although safeguards are in place that would make some of these scenarios very difficult, the range of potential cyberterrorist scenarios indicates the extent of our vulnerability.

* Power grid: Attack the computer systems that control a large regional power grid. If the power is lost for a sustained period of time, people may die. Most life support, emergency response, law enforcement, HVAC, and other systems depend on electrical power.) If a nuclear reactor is located in the region, a meltdown may occur, causing a major radiological incident that could cause mass casualties.

Fact: The U.S. power system is divided into four electrical grids supplying Texas, the Eastern States, the Midwestern States, and the Northwestern States. They are all interconnected in Nebraska. A unique aspect of the electrical grids, as with communication grids, is that most built-in computerized security is designed to anticipate no more than two disruptions concurrently. In other words, if a primary line went down, the grid would ideally shut off power to a specific section while it rerouted electricity around that problem area. If it ran into two such problems, however, the grid is designed to shut down altogether.⁷

...

* Communications systems: Invade public telephone networks, shutting down major switching hubs and disrupting emergency 911 services. Or invade the wireless networks on which we have become increasingly dependent. Extended denial-of-service could paralyze business, government agencies, airports, and some military installations.

Fact: Hackers have invaded the public phone networks, compromising nearly every category of activity, including switching and operations, administration, maintenance, and provisioning. They have crashed or disrupted signal transfer points, traffic switches, and other network elements. They have planted "time bomb" programs designed to shut down major switching hubs, disrupted emergency 911 services throughout the Eastern seaboard, and boasted that they have the capability to bring down all switches in Manhattan.

* Critical communications hubs: Disable telephone company computers that service airports, fire departments, and other communications-dependent services.

Fact: In March 1997, a hacker in Massachusetts penetrated and disabled a telephone company computer that services the Worcester Airport. For 6 hours, service was cut off to the FAA control tower, the airport fire department, airport security, the weather service, and several private airfreight companies. The lost service caused financial damages and threatened public health and public safety.

* Emergency alert and emergency response: Disable emergency alert systems, preventing the public from being notified of dangerous chemical releases or other emergencies; scramble the software used by emergency services.

Fact: A fired employee hacked into Chevron's computer systems, reconfiguring them and causing them to crash, and disabling the firm's alert system. The disabled alert system went undetected until there was a plant emergency involving a noxious release and the system could not be used to notify the adjacent community. Thousands of people in 22 States and areas of Canada were put at risk.

* Utilities: Penetrate the computer systems of utilities to cause "accidents" affecting public health and services, compromise systems monitoring the water supply, change pressure in gas pipelines to cause valve

⁷ Bowman, Stephen. When the Eagle Screams: America's Vulnerability to Terrorism. New York: Carol Publishing Group, 1994, p. 125. As quoted in Devost, Matthew G. National Security in the Information Age. University of Vermont Masters Thesis, May 1995. Accessed at: www.terrorism.com/documents/devostthesis.html.

failure, or bring down the system.

Fact: In Australia, someone penetrated a municipal computer system and used radio transmissions to create overflows of raw sewage along the coast.

...

POSSIBLE IMPACT

The potential impact of various scenarios has been described above. The vast majority of past cyberattacks have been nuisance attacks, but experts warn that attacks by true terrorists are a matter of "when," not "if." If the apparent coordination and patience employed by the September 11 terrorists were applied to a multifaceted cyberterrorist attack, the results could be catastrophic. Matthew Devost paints this hypothetical picture:

Imagine a well trained team of saboteurs, operating over several years, infiltrating several high technology companies like Microsoft or Novell, a few major automobile manufacturers, or a couple of airlines. Viruses or trojan horses are timed to detonate on a certain day, rendering computer systems inoperable. A small team of hackers infiltrates large computer, telecommunications, and power centers preparing them for denial of service attacks. Another team constructs several large EMP/T bombs and HERF Guns to be directed at targets like the Federal Reserve and Wall Street. Doomsday arrives, and the country's electronic blood stops flowing. No transfer of electronic funds, no stock exchange, no communications and power in a majority of locations, no traffic control, no air travel. . . and we have no one to blame.⁸

While this may be an extreme example, it is clear that a cyberattack of much smaller proportions has the potential for serious disruption of local networks and the systems on which emergency management depends.

...

PROTECTING AGAINST CYBERTERRORISM

In some respects, protection against cyberterrorism is a Federal and international issue. Below are some of the Federal and global actions that have been taken to help protect against cyberterrorism.

The Federal (and Global) Response

...

1996: The President's Commission on Critical Infrastructure Protection was established to analyze the vulnerabilities of and threats to critical national infrastructures, including telecommunications, electrical power systems, gas and oil storage and transportation, banking and finance, transportation, water supply systems, emergency services (including medical, police, fire, and rescue), and continuity of government. The Executive Order stated that threats include physical threats as well as threats of electronic, radio-frequency, or computer-based attacks on the information or communications components that control critical infrastructures ("cyber threats") and called for the government and private sector to work together to develop a strategy for protecting them and assuring their continued operation.

⁸ Devost, Matthew. National Security in the Information Age, p. 35.

1997: The President's Commission on Critical Infrastructure Protection concluded that the U.S. infrastructure is increasingly vulnerable to attack and that local, State, and Federal officials are not prepared to deal with the problem.

...

1998: National Security Council aide Richard Clarke was appointed head of the new office on infrastructure protection and counterterrorism. A new U.S. initiative was begun to protect telecommunications systems, banks, telephone networks, air traffic control centers, and other public and commercial networks.

2001: The Office of Homeland Security was established to integrate and coordinate counterterrorism efforts in the wake of the September 11 attacks. Its mission includes "efforts to protect critical public and privately owned information systems within the United States from terrorist attack."

...

PROTECTING AGAINST CYBERTERRORISM

System Protections

Currently there are no foolproof ways to protect a system. (A completely secure system could never be accessed by anyone.) However, three broad approaches can be used to reduce vulnerability to cyberterrorism: isolation, encryption, and security.

Isolation

Most military classified information is kept on machines with no outside connection, to prevent unauthorized access to the information. Although this method can protect certain data files, isolation is less effective in protecting a system that by its very nature requires interface with other infospheres.

Another approach that is related to isolation is the use of firewalls. Firewalls are hardware and software components that protect one set of system resources from attack by outside network users by blocking and checking all incoming network traffic. A firewall filters access to a network. It may take the form of a computer, router, or other communications device, or it may be a network configuration. A firewall defines the services and access that are permitted to each user. It screens all communications to a system, including e-mail messages (which may carry logic bombs). One firewall method is to screen user requests to check if they come from a previously defined domain or Internet Protocol (IP) address. Another method is to prohibit Telnet access into the system.

...

7. Constraints analysis: Examine requirements outside of your control, such as:

- * National and international laws.
- * Agency requirements (mission, strategy, etc.).
- * Budget.

...